

TROUBLEPROOF PROCESS INPUT AND PROCESS OUTPUTa<sup>1</sup>>

The present invention relates to a method for operating an automation system that has at least one input unit for receiving process signals and at least one output unit for driving external peripherals, the input unit and the output unit being communicatively interconnected via a bus.

a<sup>2</sup>>

To achieve rapid shutdown of the automated processes or individual operations in emergency situations when working with automation projects which are controlled and/or monitored by an automation system of this type, an emergency-stop arrangement in the form of an emergency-stop chain has ~~previously~~ <sup>conventionally</sup> been provided.

Emergency-stop switches, light gratings, tread mats or the like are integrated into such an emergency-stop chain. Due to the demands to be made on an emergency-stop arrangement, it is usually designed in conventional wiring. A tunnel furnace which is subdivided into a number of segments with respect to the automation process can be mentioned here as an example. At user-accessible positions on the outside of the tunnel furnace, emergency-stop buttons, for example, are provided for the emergency-stop arrangement, the operation of an emergency-stop button entailing, for example, the defined shutting-down of the entire process depending on the design of the overall automated system.

The emergency-stop buttons are field devices having an input function. Correspondingly, the devices shutting down the process are devices having an output function for driving external peripherals, thus, for example, output devices which control a motor for transport processes, a motor for ventilation, an hydraulic unit for positioning or the like.

In the event of an emergency-stop situation, the external peripherals must be disconnected immediately. For this

EL594604576US

purpose, an emergency-stop chain which <sup>conventionally</sup> ~~previously~~ had to be constructed in conventional wiring and which, in response to the operation of an emergency-stop button, effects an immediate shutdown of the motor or an immediate shutdown of the hydraulic unit, is set up between the input devices, that is to say, the emergency-stop buttons, and the output devices such as the motors or the units. The conventional wiring has been necessary till now due to the safety demands to be made on an emergency-stop arrangement.

In this connection, however, it is disadvantageous to provide the conventional wiring in the entire process field when working with large-area automation projects such as the tunnel furnaces described.

## SUMMARY

SUMMARY  
Therefore, the <sup>Am</sup> object of the present invention is to <sup>provide</sup> ~~specify~~ a method for operating an automation system in which it is possible to dispense with the conventional wiring for dealing with emergency-stop situations, and instead a communicative connection exists between the components of the emergency-stop chain via the bus of the automation system.

According to the <sup>present</sup> invention, therefore, the conventional wiring for the emergency-stop arrangement is omitted, and all field devices, i.e., thus also the emergency-stop buttons and the motors or units to be integrated into the emergency-stop chain, are communicatively connected via the process bus.

This objective is achieved for a method for operating an automation system, wherein the automation system has at least one input unit for receiving process signals and at least one output unit for driving external peripherals, and wherein the at least one input unit and the at least one output unit are communicatively interconnected via a bus, in that at least one of the input units and at least one of the output units are constructed as a failsafe input unit and as a failsafe output unit, respectively, ~~that the~~ <sup>the</sup> failsafe input unit transmits a data item to the failsafe output unit at predetermined times,

that the data item includes at least one useful information item, one destination point code designating the addressed output unit and one origin code designating the transmitting input unit, ~~that the~~ <sup>The</sup> output unit interprets the continuous reception of the data item as an indication of an intact communication relationship, and otherwise shifts the connected peripherals into a safe state.

According to the <sup>present</sup> invention, the safety demands to be made on an emergency-stop arrangement are met if the input devices, i.e., for example, the emergency-stop buttons and the output devices that are to be integrated into the emergency-stop chain and are provided for driving the motors or units, are in each case constructed to be failsafe. In the event of an emergency-stop situation, the following sequence then occurs in the automated system:

In response to the operation of an emergency-stop button, a data item is placed on the bus by the data input device.

According to the specifications of the bus protocol used for the physical communications link, the data item to be transmitted includes at least one useful information item, in this case therefore the information as to whether the emergency-stop button has been pressed or not, at least one destination address, i.e., the address of the communication partner to which the message is sent - a special identifier enabling the message to be sent to all communication partners - and, finally, the origin code which identifies the sender of the data item.

The <sup>present</sup> invention can then be used, on the one hand, in such a manner that the data item is sent to a quite specific communication partner, the addressee recognizing from the destination address contained in the data item that the data item is intended for it, or the data item is sent to all communication partners, each individual communication partner determining from the origin address of the data item whether the data item, i.e., the useful information in the data item,

is to be evaluated by it.

On the other hand, the data item can also be sent to a higher-level unit of the automation system, e.g. the central

5 processing unit of a programmable controller, the latter in turn recognizing from the origin code of the data item that a message, e.g., from an emergency-stop button, has arrived which needs immediate handling, so that immediately after detecting the data item, the central processing unit forwards it to the  
10 output devices so that they trigger a deceleration or shutdown of the motors or units connected to the output devices, or they themselves transmit a further data item to the output devices which leads to the same result.

15 In this context, the output unit interprets the continuous reception of the data item from the input unit as indication of an intact communication relationship. In the case when the output unit detects that a data item from an input unit fails to appear during a time span which is greater than a  
20 predeterminable time span, the output unit shifts the connected peripherals into a safe state and thus ensures again that the connected motors or units are shut down.

For use within the framework of the method according to the  
25 <sup>present</sup> invention for operating an automation system, provision is also made for a failsafe data input device having at least one input channel for connecting peripheral sensors, the data input device being provided with a test circuit which triggers a test procedure at predetermined times and, in so doing,  
30 effects a status change for at least one of the input channels of the failsafe input device, an internal logic monitoring the status change and, if necessary, outputting an error message, the status change effected by the test circuit being canceled again at the end of the test procedure, and the test procedure  
35 being completely transparent for reading out the affected input channel.

Furthermore or as an alternative, a failsafe data input device

having at least one input channel for connecting peripheral sensors, in which the at least one input channel is designed to be antivalent, is provided for use within the framework of the method according to the invention for operating an  
5 automation system.

Due to the above-mentioned measures, i.e. due to the antivalent design of the input channel or due to the monitoring of the input channel by a test circuit, the  
10 failsafe input devices designed in accordance with the above description become failsafe data input devices, it also being possible to combine the two measures.

Furthermore, an output unit constructed as a failsafe output  
15 device is provided for use within the framework of the method according to the <sup>present</sup> invention for operating an automation system. If a processing unit for processing user-designable logic operations is provided for the failsafe data output device, where the processing unit evaluates the useful information of  
20 a received data item, subjects the useful information to the user-designable logic operation and drives the at least one output channel in accordance with the result of the logic operation, software components which were previously usually provided in a higher-level automation device, e.g., the central  
a 25 processing unit of a programmable controller, are also displaceable into the failsafe output device, so that in this case especially fast and effective processing and evaluation of the logic operations is possible.

30 If for the failsafe data output device, the processing unit furthermore or alternatively monitors the time sequence of the process data transmitted with the useful information and drives the at least one output channel only if the time sequence of the data required for driving the output channel  
35 lies within predeterminable tolerances, then a so-called muting is possible which contributes to increasing the reliability of the automated process. The protection of a traverser with the aid of an inductive limit switch and a

light barrier can be named as an example. When the traverser moves, it triggers both the inductive limit switch and the light barrier in a certain time sequence determined by the speed of the traverser.

5

When the time sequence of the input of the associated signals is within the predetermined tolerances, the processing can be continued. On the other hand, a person only triggers the light barrier when the additional signal of the inductive  
10 limit switch is absent during the predetermined tolerance time. Such a constellation can be evaluated as an alarm constellation, to which reaction is possible with an emergency-stop arrangement.

15 If the failsafe data output device is provided with a monitoring circuit, constructed as watchdog and monitoring the processing unit, which shifts the at least one output channel into a safe state as soon as a malfunction of the processing unit is detected, then a second disconnect path is established  
20 via the monitoring circuit constructed as watchdog. If, for example, the processing unit were no longer capable of disconnecting a special output, then a motor or a unit, for example, would remain permanently activated without the monitoring circuit. The monitoring circuit constructed as  
25 watchdog detects such states and, upon detecting, switches the outputs into a safe state.

If, in the failsafe data output device, the output channel, which can be driven by the processing unit, is constructed as  
30 a readback output channel, if the signal which can be supplied to the output channel can also be supplied to the monitoring circuit, and if the monitoring circuit compares the signal supplied to it and the signal read back from the output channel and, in response to deviations, shifts the affected  
35 output channel or even all the output channels and the peripherals connected thereto into a safe state, then discrepancies in the driving of the respective output channels are detected and they are immediately shifted

into a safe state.

ans.  
a3  
a3>

~~Other features, advantages and possible applications of the~~

5 present invention come to light from the subclaims, the following description of exemplary embodiments with reference to the drawing, and the drawing itself. In this context, all features described and/or represented pictorially, alone or in any combination, form the subject matter of the present  
10 invention, regardless of the way in which they are combined in the patent claims or their antecedents. In the drawings

Figure 1 shows a simplified block diagram of an automation system!.

15 Figure 2 shows a block diagram of a failsafe data input device! and .

Figure 3 shows a block diagram of a failsafe data output device.

ans.  
a4  
a4>

20 In Figure 1, a block diagram of a simple automation system having a failsafe data input device 2, a failsafe data output device 3 and a higher-level automation device 1, e.g., central processing unit 1 of a programmable controller, is shown by way of example. The devices are communicatively interconnected  
25 via a bus 4, preferably via a bus 4 suitable for use in industrial environments, especially the profi process field bus 4.

Failsafe data input device 2 is connected to an emergency-stop  
30 button 1'. Failsafe data output device 3 is connected to a motor 2'. When emergency-stop button 1' is operated, data input device 2 receives this signal, transmits it via bus 4 to data output device 3 which thereupon effects the shutdown of motor 2'.

35

Figure 2 shows a block diagram of a first embodiment of a failsafe data input device 2. Failsafe data input device 2 is communicatively connected via bus 4 to other devices 1, 2, 3

linked to bus 4, the bus interface being effected by a bus ASIC 5. The functions of data output device 3 are effected by a processing unit 6 which, for example, is an ASIC or a microprocessor. Input channels 7-0, 7-1...7-7 are supplied 5 directly or indirectly to processing unit 6.

Also provided in data input device 2 is a test circuit 8 which is likewise controlled by processing unit 6 and which triggers a test procedure at predetermined times and, in so doing, 10 effects a status change for at least one of input channels 7-0, 7-1...7-7 of failsafe data input device 2. This status change is monitored by an internal logic 9 which outputs an error message if the status change triggered by test circuit 8 has no effect on the status of the respective input channel 7-15 0, 7-1...7-7. At the end of the test procedure, the status change effected by test circuit 8 is canceled again. In this context, the test procedure is completely transparent for reading out the affected input channels 7-0, 7-1...7-7 during normal 20 operation of failsafe data input device 2.

Furthermore, if inputs 7-0, 7-1...7-7 are also supplied in negated form 7-0', 7-1'...7-7' to processing unit 6, the input channels are designed to be antivalent. Processing unit 6 then 25 reads the status, e.g. logical 0, for the input channel in question, e.g. 7-2, and as negated status for antivalent corresponding input 7-2', the corresponding complement, thus logical 1 in this case. Malfunctions during the forwarding of the statuses of the respective input channels can then be 30 detected simply and reliably by processing unit 6 by checking in each case whether complementary statuses are present on the respective input channel and on the input channel antivalent thereto.

35 Figure 3 shows a block diagram of a failsafe data output device 3 which is connected to process bus 4 by a bus ASIC 14 constructed as bus interface 14. Failsafe data output device 3 has a processing unit 10 for processing user-designable logic



operations, processing unit 10 evaluating useful information TN of a message received via process bus 4, subjecting useful information TN to the user-designable logic operation and driving the at least one output channel 11-0, 11-1... 11-7 in accordance with the result of the logic operation.

In the illustration according to Figure 3, failsafe data output device 3 has a monitoring circuit 12 constructed as watchdog 12 and monitoring processing unit 10, said monitoring circuit shifting the at least one output channel 11-0, 11-1...11-7 into a safe state as soon as a malfunction of processing unit 10 is detected. For this purpose, monitoring circuit 12 monitors the functioning of processing unit 10, the statuses of the respective output channels 11-0, 11-1... 11-7 being determined by monitoring circuit 12 in the event processing unit 10 malfunctions, for which purpose a driver circuit 13 is provided which can be driven both by processing unit 10 and by monitoring circuit 12.

If processing unit 10 malfunctions, the driving, output by monitoring circuit 12, of the respective output channels 11-0, 11-1...11-7 overwrites the respective driving by processing unit 10 which has already been detected as faulty at this time.

25

In the illustration according to Figure 3, failsafe data output device 3 is also constructed in such a manner that output channel 11-0, 11-1... 11-7, which can be driven by the processing unit, is constructed as readback output channel 11-0', 11-1'... 11-7', that the signal which can be supplied to output channel 11-0, 11-1...11-7 can also be supplied to monitoring circuit 12, that monitoring circuit 12 compares the signal supplied to it and signal 11-0', 11-1'...11-7' read back from the output channel and, in response to deviations, shifts the affected output channel 11-0, 11-1 ...11-7 into a safe state.

In the above description, the assumption is always input and output devices 2, 3 having in each case eight input and output channels, respectively. Naturally, the number of channels can also be greater or less than eight, e.g., 16 or 32.